DEPARTMENT OF THE ARMY
HEADQUARTERS, 4th INFANTRY DIVISION
FORT HOOD, TEXAS 76544-5200

AFYB-CG

22 March 2007

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: 4ID, G6 Information Assurance (IA) Policy # 14: IA Alert and Reporting Procedure

1. References

a. AR 25-1, Army Knowledge Management and Information Technology, 15 July 2005.

b. AR 25-2, Information Assurance, 14 November 2003.

c. HQDA CIO/G6 Information Assurance Vulnerability Management Program, Army Information Assurance web page, https://informationassurance.us.army.mil

d. Army Policy for the Implementation of the Information Assurance Vulnerability (IAVA) Process, https://www.acert.1stiocmd.army.mil/policy/Army_IAVA_Policy.txt.

2. Purpose: The purpose of this policy is to ensure that IA alerts are disseminated to all parties affected in a timely and efficient manner and that required reports are provided to the correct parties in a timely and efficient manner. This procedure does not apply to Information Assurance Vulnerability Alerts (IAVA). IA alerts of any type, other than IAVA, from any source, will be reported to the 4ID IA Team at DSN 737-0785, immediately. Alerts may come from agencies outside of the area serviced by 4ID, such as EUR-TNOSC, RCERT-E, ACERT, etc. Alerts may also come from 4ID supported activities or from with-in the 4ID structure itself. An alert can be anything from sudden computer virus activity affecting several machines to suspected compromise of a machine.

3. Applicability: This policy is applicable to all United States military personnel, and to civilians serving with, employed by, or accompanying the Armed Forces of the United States, while assigned to the 4th Infantry Division or while present in the 4th Infantry Division's AOR who plan, deploy, configure, operate, and maintain Automated Information Systems (AIS) directly or indirectly attached to 4ID networks.

4. Responsibilities:

a. 4ID Information Assurance Manager (IAM) will:

(1) Ensure the IAVA alerts and reports are implemented throughout the 4ID area of responsibility.

(2) Determine the required response and direct the 4ID IA Cell to forward the alert, with any necessary amplifying instructions and information to their subordinate IASO/SA(s), if any, with information as directed.

(3) Report as directed by the particular alert. The IAM(s) will receive reports from their subordinate IASO/SA(s). Report contents will vary based upon the specific alert, but will almost always contain details of what was scanned/blocked, the results of scanning or blocking, to whom the affected devices belong, the number of affected devices, and the status of corrective actions. Report frequency will vary as well, but as a minimum will be as often as significant changes occur. Some alerts will come with reporting content, formats, and frequencies specified. Those requirements will be met with additional updates as required. All reports will contain enough detail to fully describe the situation: who and what is/was affected, when; where it is; and what is

being done about it. The details required will be as fluid as the situation and may change drastically and often.

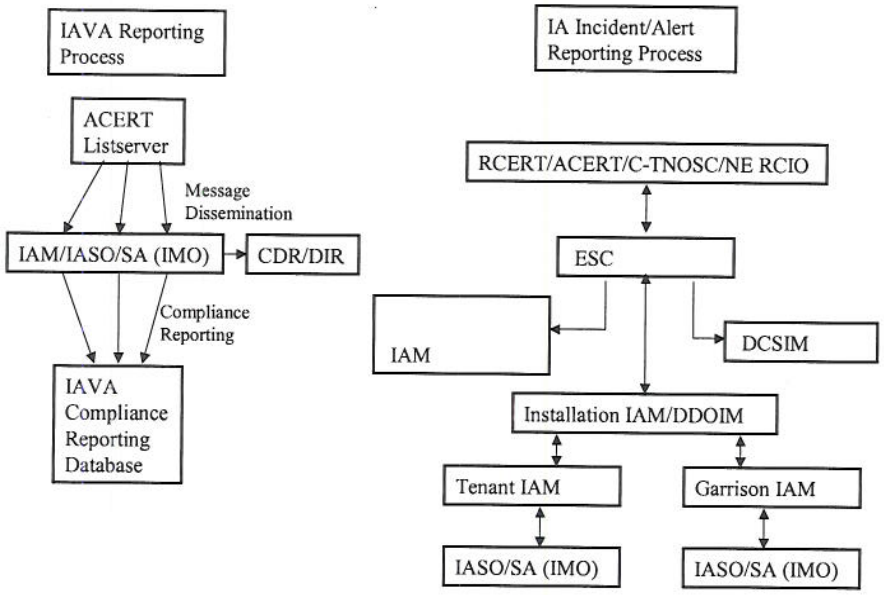
b. 4ID IA Team will take action immediately on those alerts that indicate that network scanning and/or specific machine or port blocking are required. Report activities to the 4ID IAM as they are initiated, when significant status changes occur, and when they are complete.

c. Unit/Section IASO/SAs will:

(1) Ensure the IAVA alerts and reports are implemented throughout their area of responsibility.

(2) Report as directed by the 4ID IAM.

IA IAVA, Incident, and Alert Reporting



5. The primary method of reporting will be via email, unless otherwise directed. In a case where email is unavailable, or time constraints or the situation make email impractical, reports can be made by voice. Follow-up written reports may be required to catch misunderstandings/errors induced during the voice transmission and to provide a durable record.

6. POC for this policy is the 4ID Information Assurance at DSN 737-0785 or commercial 254-287-0785.

JEFFERY W. HAMMOND
MG, USA
Commanding